ABSTRACT

An apparatus and method is disclosed for establishing a one-time cryptographic pad between a communicating pair, a communicating pair comprising a pair of transmitter-receivers, each of the pair having a plurality of cryptographic devices in common. The communicating pair also store previously exchanged messages and transmissions, a transmission comprising secure data exchanged by the pair that is independent of message content. The first transmitter-receiver randomly selects a cryptographic device and a previous transmission or message that has been sent to the second transmitter-receiver. The first transmitter-receiver also randomly selects a reference to a message or transmission previously sent by the second transmitter-receiver. The first transmitter-receiver encrypts the previously sent transmission or message and the reference to the message or transmission previously sent by the second transmitter-receiver and sends to the second transmitter-receiver. The second transmitter-receiver discovers the encryption device used by the first transmitter-receiver, verifies the message or transmission sent by the first transmitter-receiver, and uses the decrypted reference to access the previously sent transmission or message, then uses the discovered encryption device to encrypt the previously sent transmission or message and sends to the first transmitter-receiver. The first transmitter-receiver decrypts the transmission or message previously sent by the second transmitter-receiver, and authenticates. If authentication is successful, the first transmitter-receiver encrypts using the randomly selected cryptographic device.